INL/CON-08-14059
PREPRINT

Fully Integrating the Design Process

8th International Conference on Facility Operations – Safeguards Interface

T. A. Bjornard
R. S. Bean

March 2008

FULLY INTEGRATING THE DESIGN PROCESS

T.A. Bjornard and R.S. Bean

Idaho National Laboratory, Nuclear Nonproliferation Division, 2525 N. Fremont Ave., Idaho Falls, ID 83415-3740
Trond.Bjornard@inl.gov, Robert.Bean@inl.gov

ABSTRACT

The basic approach to designing nuclear facilities in the United States does not currently reflect the routine consideration of proliferation resistance and international safeguards. The fully integrated design process is an approach for bringing consideration of international safeguards and proliferation resistance, together with state safeguards and security, fully into the design process from the very beginning, while integrating them sensibly and synergistically with the other project functions. In view of the recently established GNEP principles agreed to by the United States and at least eighteen other countries, this paper explores such an integrated approach, and its potential to help fulfill the new internationally driven design requirements with improved efficiencies and reduced costs.

Key Words: Safeguards by Design, Fully Integrated Design Process, Intensity of Effort

INTRODUCTION

The statement of principles for the Global Nuclear Energy Partnership (GNEP) has now been officially endorsed by eighteen or more countries, including the United States (U.S.). The overarching mission of this international movement is to support the global growth of nuclear energy while reducing nuclear security risks.[1]

Included are risks associated with state level threats that would manifest in the acquisition by a country of weapons-usable nuclear materials from either declared or undeclared activities. Proliferation resistance is one defense against these state level threats, and is defined as "those characteristics of a nuclear energy system that impede the diversion or undeclared production of nuclear material or misuse of technology by the state seeking to acquire nuclear weapons or other nuclear explosive devices." [2] Additionally, the GNEP defenses include strict observance of present and enhanced IAEA safeguards, UN Security Council Resolution 1540, and maintaining the highest levels of nuclear safety and physical security. State safeguards and security, such as those specified by DOE Order 470.4 are the defenses against subnational threats such as terrorism, theft and sabotage that would be carried out by a subnational adversary – an individual or group, including potentially some form of 'insider.' [3]

Defenses against 'natural hazards' are the domain of safety, which is also emphasized by GNEP. Thus, the GNEP vision requires effective defenses against essentially all threats, whether natural or man-made in origin.

The 2002 Como II conference usefully considered the nature of the steps that might be undertaken to strengthen proliferation resistance of a nuclear energy system.[2] The team defined intrinsic features as those that result from the design of the nuclear system, including those that enable the efficient application of extrinsic measures. The PRPP group subsequently expanded this definition, noting that intrinsic features include inherent physical properties of the system, and are in general very robust and desirable because they are very difficult to modify or overcome.[4] Extrinsic PR measures are associated with the states' decisions and undertakings - examples include treaties, commercial and legal arrangements, export controls, or actions to support UN Resolution 1540, and they include the application of international safeguards. Thus PR measures are intrinsic or extrinsic, and they may be technical or institutional in nature.

Some very effective intrinsic PR features can be implemented at the highest level of the global fuel cycle architecture. Examples would include the selection of the fuel cycle itself, e.g. uranium and/or plutonium fuels, once through or a specific recycling process, and the use and deployment of uranium enrichment. Other examples are those GNEP features that seek at the highest level to avoid or minimize the spread of nuclear materials and technologies of interest to potential proliferators. The effectiveness of such features can be illustrated through the risk equation. The risk from a threat is defined as being equal to the product of the probability that an event will take place, times the probability that the event will produce a given consequence. (Note that, by

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-Rom, Danielle Peterson, Pacific Northwest National Laboratory, P. O. Box 999, K8-16, Richland, WA, 99352 (2008)

definition, the proliferation risk is zero in the case of a nuclear weapons state using its own technology or material, because they cannot 'proliferate' to themselves.) High level intrinsic features can make a particular proliferation event less likely, or can cause the state to attempt a path that is more prone to failure. Either way, the product of the risk equation, and thus the proliferation risk, is reduced.

Additionally, intrinsic PR features can be implemented at the level of the nuclear facility design. Examples include features that would make it very difficult or impossible to divert nuclear material without being detected. Another very important example would be design features that facilitate transparency and verification at the international level, or rather, features that enhance safeguardability. Safeguardability is defined as "the ease with which a system can be effectively and efficiently put under international safeguards." [4] Thus, it is clear that to strengthen the defenses against proliferation at the level of the nuclear fuel cycle facility, emphasis must be given in the facility design process to the identification and incorporation of intrinsic design features for proliferation resistance and physical protection, as well as features that will enhance the cost effective application of both international and state safeguards. The modern challenge is to meet all of these requirements in an integrated, synergistic and cost effective manner.

A NEW INTEGRATION CHALLENGE

In order to fulfill the GNEP vision a modern fuel cycle facility must fulfill internationally driven requirements such as proliferation resistance and incorporation of international safeguards, in addition to fulfilling the state level requirements for safety, safeguards and physical security required by the host state. In the case of the U.S. this represents a *de facto* change in practice, since, historically, international safeguards have not been routinely applied to nuclear facilities in nuclear weapons states, and nonproliferation considerations have become dramatically more urgent in recent years because of the changing threat concerns and the global nuclear renaissance. Additionally, perhaps for the reason that few new domestic nuclear facilities have been built in recent decades, the current environment that anticipates new nuclear construction in the U.S. is driving what appears to be a dynamic process with regard to updating state safety and safeguards, and possibly also security approaches. Much progress has been made in many fields since nuclear construction was thriving in the U.S. some 20 to 30 years ago – in a then very different threat environment - and it is useful and important to examine all practices from the perspective of the latest standards.

FULLY INTEGRATED DESIGN PROCESS

Figure 1 illustrates the integration challenge that is presently posed by the design of a new nuclear facility within the U.S. DOE system, when the international considerations of proliferation resistance and international safeguards are included.

At the bottom of Fig. 1 are the bulk of the 'usual design activities' for a project, including process design, instrumentation and controls, facility and equipment layout, and so forth, but as defined in this figure, specifically excluding those matters relating to safety and nuclear security. These activities are prescribed in DOE documents, and in the case of a capital construction project are governed by a DOE order.[5] Included at the top of Fig. 1 is the ongoing safety related development being driven by the U.S. DOE Integrated Safety Management program, to emphasize and formally codify the inclusion of Safety in Design in the design process for nuclear facilities. The effort has resulted in the publication of a draft standard, U.S. DOE Standard 1189, "Integration of Safety into the Design Process." [6]

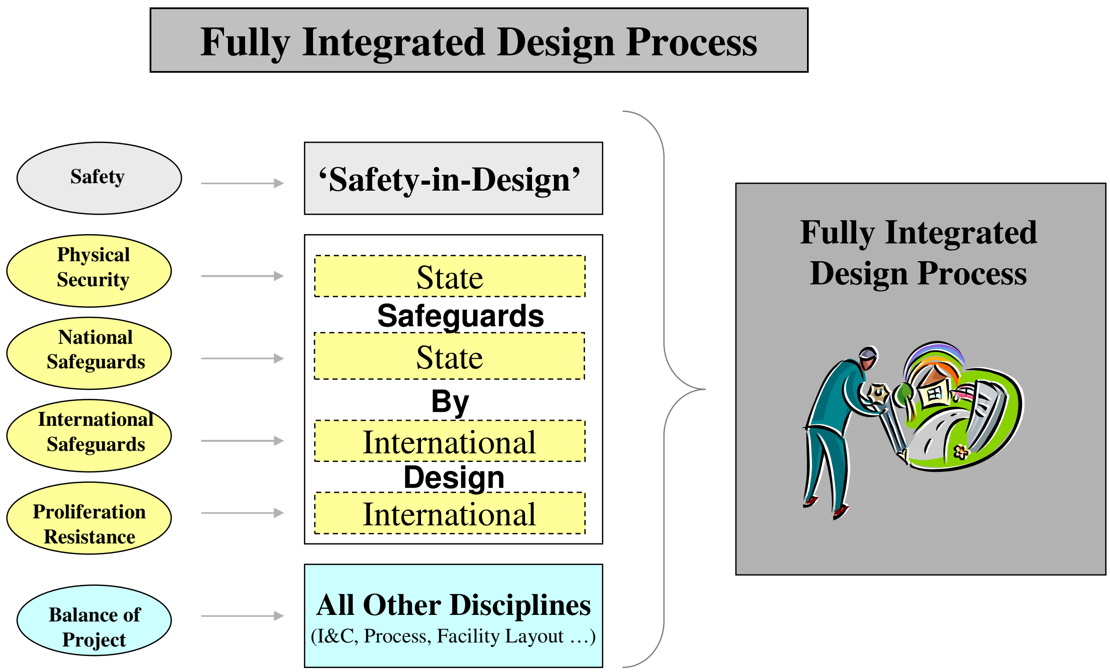


Figure 1. The Fully Integrated Design Process.

The yellow boxes included in the center of Fig. 1 focus the discussion on the design activities to mitigate nuclear security threats (from both state and subnational actors). The orders, guides and manuals covering DOE Safeguards and Security address the requirements and activities associated with defining and defending against the subnational threats, notably this includes the application of DOE Material Control and Accounting (safeguards) and physical protection of nuclear materials, as well as some other items such as personnel, cyber, and information security.[7]

The lower two yellow boxes represent the activities to defend against proliferation. The specific implementation of international safeguards in the case of projects in the U.S. would presumably be based on the standard IAEA safeguards approaches, while

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-Rom, Danielle Peterson, Pacific Northwest National Laboratory, P. O. Box 999, K8-16, Richland, WA, 99352 (2008)

accounting for the specifics of U.S. agreements with the IAEA through the Comprehensive Safeguards Agreement (CSA) and Additional Protocol (AP).[8] It is useful to note that the activities to support international safeguards include consideration of both intrinsic design features that would enhance safeguardability, as well as the application of extrinsic measures that would be required for independent verification in a completed facility.

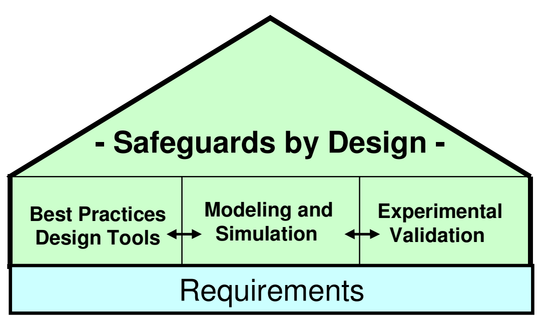
SAFEGUARDS BY DESIGN

In the center of Fig. 1, a larger concept has been introduced that spans proliferation resistance, international safeguards, and state safeguards and security. This is the concept of 'Safeguards by Design', which we define further via Fig. 2 as, "the inclusion of proliferation resistance, international safeguards, state safeguards and physical security, as full and equal partners in the design process." [9] Essentially Safeguards by Design (SBD) puts all design matters relating to nuclear security under one hat. The fully integrated design process is then one which integrates safety and SBD into the context of a larger project.

The foundation upon which SBD is conducted is defined by the full set of requirements and success criteria (metrics by which one can assess fulfillment of a requirement) for the project. The SBD process includes the activities by designers to apply know-how, tools, and models – including supporting experimental data – in the context of a nuclear facility design project.

<u>'Safeguards By Design'</u>

"The integration of safeguards, physical protection and proliferation resistance as full and equal partners in the design process of a nuclear energy system or facility."



Early focus and contribution by expert teams

Figure 2. Safeguards by Design.

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-Rom, Danielle Peterson, Pacific Northwest National Laboratory, P. O. Box 999, K8-16, Richland, WA, 99352 (2008)

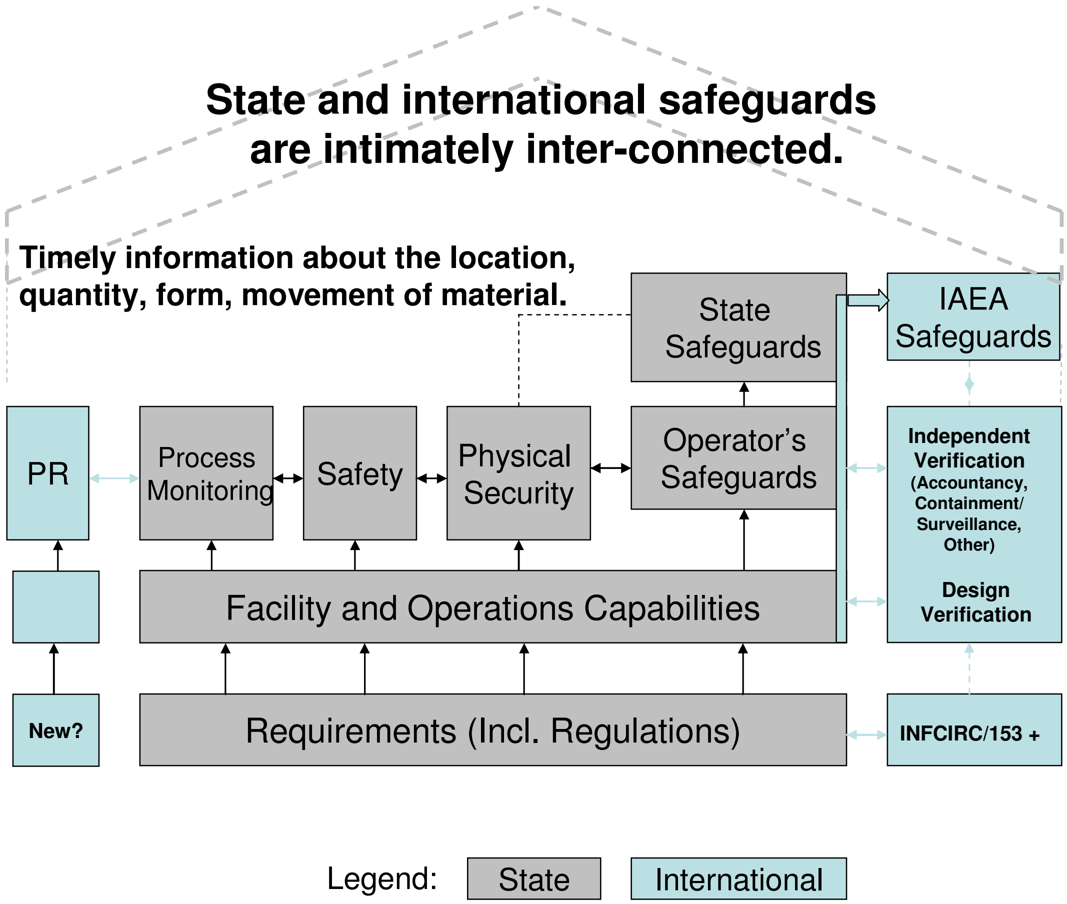


Figure 3. State and international safeguards, as well as many other operations of a nuclear facility depend on the same requirements foundation.

The Como II discussions in 2002 articulated the high level fundamentals of proliferation resistance, defined a new vocabulary for nonproliferation, and also foresaw the methodological approaches that should be developed and used to define and assess the robustness of nuclear energy systems of the future.[2] The Como II team suggested a three pronged approach to methodology for PR, to include a checklist, and qualitative and quantitative assessment approaches. It is notable that in the ensuing years substantial progress has been made towards developing methodologies for all three of these approaches. The IAEA led INPRO program has followed the checklist approach, which has been developed to the point where it has been used in the assessment of the DUPIC fuel cycle.[10, 11] The Generation IV International Forum (GIF) established an international working group that has been developing a risk-based approach to the qualitative and quantitative assessment of the relative PR and physical protection robustness of alternative nuclear energy systems.[4] The current application of these two alternative methodologies to example and real world problems may well form the basis for informing future revisions of these methodologies. While these approaches should not yet be considered fully mature, there is mounting evidence that they can be usefully applied to real world problems, both at the global architecture level as well as at the facility design level.

Two further observations should be made regarding Fig. 3. First, it should be noted that the functions specifically mentioned are all very much concerned with tracking nuclear material, though perhaps for different reasons. The second observation relates to the strong interdependence of state safeguards and the international safeguards. This highlights the importance of considering them together in a project, as opposed to treating the international safeguards as an independent 'add on.'

THE DESIGN PROCESS

Consideration of the nature of the design process itself will be useful in informing approaches to this new, integrated design problem.

Figure 4 illustrates notionally how the intensity of the design activity changes as the project progresses. First of all, it should be noted that the foundation for all of the activities - and the yardstick against which to measure their worthiness – is comprised of the formal requirements and success criteria that have been established for the project. It is essential that a design project begin with the complete and clear specification of all relevant requirements, and that success criteria be developed and agreed upon that define the objective measures by which one assesses fulfillment of the requirements. The modern GNEP design problem will require establishing new requirements and criteria where current U.S. regulations and practices are silent, most notably for proliferation resistance, if it is to be included in a project. A complete and clear statement of measurable requirements is essential.

The second important observation is reflected in the curve representing the application of expert know-how. In the case of a DOE project this early portion of the project might represent the project initiation and pre-conceptual or conceptual design phases. At this early stage of the project, the project team is wrestling with fundamental questions such as mission need, as in, "Does it make sense to pursue a facility like this at all?" Design details may be few and far between, and if they exist they are likely to be fairly high level considerations on the order of, "Should we build a 1,000 MWe nuclear power reactor?" During the following conceptual design phase, the design team is seeking to establish alternative approaches to meeting the mission requirements, and to identify cost and risk ranges for the alternative approaches. Again, only high level information may be available, and the designers are dealing with scoping type questions such as, "Should this be a PWR, BWR or VHTR?"

Nature of Facility Design Activity

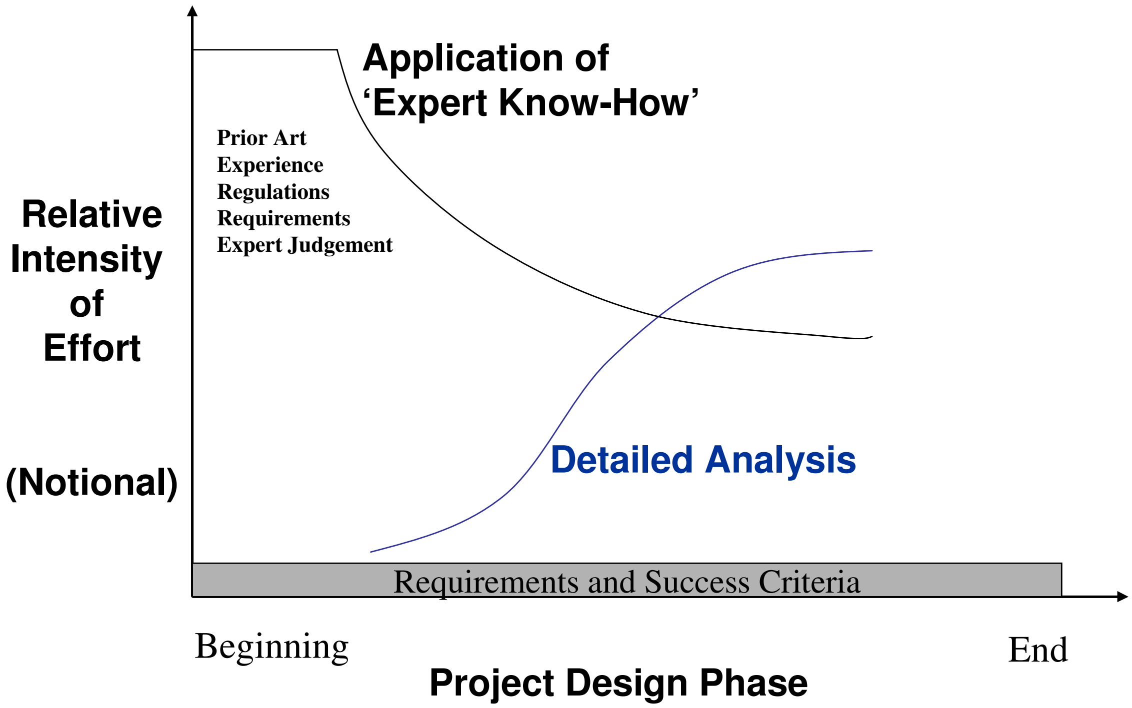


Figure 4. Relative intensity of effort during the design process.

A salient observation is that in the earliest project stages it is the application of know-how by the expert design team members that is the most important contributor. This is why it is absolutely essential that the important project requirements are represented by experts from the very beginning of the project. Next to defining a clear and measurable project requirement for 'Factor X,' perhaps the single biggest contribution one could make to the cost-effective success of 'Factor X' in a project would be to have a 'Factor X' expert participate fully in the project from the very beginning. He would contribute to the mission need phase, as well as the drafting of the project's Functional and Operational Requirements document that essentially defines the project. Such considerations are included in the DOE approach to safeguards and security as articulated in the published 413.3A series of documents, as well as in the standard being developed for safety-in-design.[5, 7, 12] The fully integrated design process should therefore include experts in nonproliferation and international safeguards as members of the design team, from the very beginning, together with their safeguards and security teammates and the rest of the project team. They should cooperate closely with the other disciplines detailed in Fig. 3.

The third important observation from Fig. 4 is represented by the curve labeled 'detailed analysis.' It is an interesting conundrum that it is at the earliest stages of the project that one has the opportunity for the greatest beneficial impact through the establishment

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-Rom, Danielle Peterson, Pacific Northwest National Laboratory, P. O. Box 999, K8-16, Richland, WA, 99352 (2008)

of intrinsic design features at the lowest cost, and yet, it is precisely at this stage that the fewest design details are known. This further underscores the importance of the early and full participation of relevant experts. Also, it points to the usefulness of higher level design tools that can provide meaningful direction in the absence of specific detail. A higher level checklist or qualitative approach may be very useful at this stage, such as a qualitative application of the PRPP methodology, as well as the application of higher level modeling and simulation to explore alternatives.

It is only as further details become available that other detailed analysis techniques can be usefully employed. As new and improved tools are developed to aid in the assessment of proliferation resistance, safeguardability, physical protection and state safeguards they will find useful and increasingly intense application in the process. In a project sense, they will increasingly reduce the intensity of expert know-how and replace it with detailed analysis.[13, 14]

CONCLUSIONS

The challenge for an integrated design process is to effectively and efficiently incorporate international safeguards, proliferation resistance, and nuclear security and safeguards into the entire design effort from the very beginning. Successful integration will include:

- Early and continued involvement of appropriate experts (physical security, state safeguards, international safeguards, proliferation resistance, etc.) in the design process,
- Early, complete, and clear establishment of the requirements and success criteria,
- Strong encouragement to identify intrinsic facility features early in the design process,
- Strong encouragement to develop synergistic, cross-discipline design solutions,
- Meaningful cost analysis to balance near term investment in intrinsic features versus long term investment in extrinsic (operating) costs,
- Development of standards and guidance to assist establishment of requirements and direct the inclusion of tools and analysis techniques, and
- Identification of extrinsic features (at the facility and higher level).

As countries prepare to build new nuclear fuel cycle facilities, there must be a complementary preparation to advance and improve the safeguardability of those facilities. Fully integrating state safeguards and security, international safeguards, and proliferation resistance into the overall design process will enhance the cost effectiveness of providing for nuclear security, and increase the efficacy of those same measures.

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-Rom, Danielle Peterson, Pacific Northwest National Laboratory, P. O. Box 999, K8-16, Richland, WA, 99352 (2008)

REFERENCES

1. United States Department of Energy, “GNEP Statement of Principles,” http://www.gnep.energy.gov/pdfs/GNEP_SOP.pdf, September 16, 2007.
2. IAEA Department of Safeguards, “Proliferation Resistance Fundamentals for Future Nuclear Energy Systems,” STR-322, December 2002.
3. United States Department of Energy, “Safeguards and Security Program,” DOE O 470.4, August 2007.
4. Generation IV International Forum/PRPP Expert Group, “Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, Revision 5,” GIF/PRPPWG/2006/005, November 30, 2006, printed by the OECD Nuclear Energy Agency for the Generation IV International Forum.
5. United States Department of Energy, “Program and Project Management for the Acquisition of Capital Projects,” DOE O 413.3A, July 27, 2006.
6. United States Department of Energy, “DOE Standard – Integration of Safety into the Design Process,” DOE-STD-1189-2007, March 2007.
7. United States Department of Energy, “Safeguards and Security Program Planning and Management,” DOE O 470.4-1, March 2006.
8. International Atomic Energy Agency, “The Structure and Content Of Agreements Between the Agency and States Required In Connection With The Treaty On The Non-Proliferation of Nuclear Weapons,” INFCIRC/153 (Corrected), June 1972.
9. Bjornard, T. and Pasamehmetoglu, K., “SESAME - Advanced Modeling and Simulation Applied to Nuclear Nonproliferation and Safeguards,” INMM 47th Annual Meeting, Nashville, Tennessee, June 2006.
10. International Atomic Energy Agency, “Methodology for the assessment of Innovative Nuclear Systems: report of Phase 1B (first part) of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO),” IAEA TECDOC 1434, December 2004.
11. Yang, M.S. and Park, J.H., “Korean Assessment of the Proliferation Resistance on the Whole Fuel cycle of DUPIC,” Revision 1, Korea Atomic Energy Research Institute, February 18, 2006.
12. United States Department of Energy, “Safeguards and Security for Program and Project Management:,” DOE G 413.3-3, November 15, 2007.
13. McCormack, Amy, “Safeguards First Principles Initiative (SFPI) Evaluation Tool: COMPASS,” INMM 48th Annual Meeting, Tucson, Arizona, July 8 – 12, 2007.
14. Elwood, Robert, et al, “Nuclear Material Control and Accountability (MC&A) Functional Model and MC&A System Effectiveness Tool (MSET),” INMM 48th Annual Meeting, Tucson, Arizona, July 8 – 12, 2007.